SETI

Servizi e Tecnologie per l'Informatica

Noventa Padovana, 15/11/2021

File e versione: 20211115_relazione_Ads.odt

Spett.le Comune di Veggiano

Alla C.A. dell'Assessore all'Informatica
Alla C.A. del Responsabile dell'Informatica

OGGETTO: relazione Amministratore di Sistema

Gentili Signori

anticipo questa relazione in qualità di Amministratore di Sistema per portarvi alla conoscenza dello stato del sistema informatico comunale e degli interventi eseguiti nell'ultimo anno di attività.
Per dare una migliore lettura ho suddiviso gli argomenti per tipologia omogenea, cercando di esporli in modo comprensibile

1 **Datacenter/Server di produzione**

Il locale datacenter è ordinato ed in sicurezza ed è presente un buon sistema di UPS e di climatizzazione.

Il server di produzione è stato sostituito con un server DELL di ultima generazione con copertura di manutenzione e garanzia di 5 anni.

Il nuovo server permetterà all'Ente di avere risorse elaborative buone per i prossimi anni ed ha la possibilità di essere ampliato a livello elaborativo per future esigenze.

Lo storage interno è stato ottimizzato razionalizzando le VM di produzione ed ora ha uno spazio idoneo per la gestione corrente.

Lo storage acquisito nel nuovo server è stato configurato in modo da avere uno storage SSD ad alte prestazioni dedicato esclusivamente ai Gestionali ed un secondo storage con larga capacità e buone prestazioni dedicato al documentale ed alle esigenze di archiviazione.

La RAM è ottimale per l'attuale struttura e per le necessità di elaborazione.

Il Sistema Operativo Microsoft Windows Server è stato aggiornato all'ultima versione disponibile 2019 ed il sistema di virtualizzazione VmWare è coperto da assistenza ed aggiornato all'ultima versione disponibile.

Nell'ottica di una migliore sicurezza è stata eliminata dal locale ced ogni componente cartaceo presente (pacchi di carta per fotocopiatore depositati), e spostata in altro locale la fotocopiatrice presente al fine di limitare l'accesso al locale solo alle persone incaricate e di permettere l'adeguato funzionamento del sistema di condizionamento.

SETI snc
Sede operativa: 35027 Noventa Padovana Via Panà, 56/B tel. 049 0990006 fax 049 0990007
PEC: seti@legalposta.it - mail: posta@setiweb.it - WEB: www.setiweb.it
C.F. e P.IVA 01281420297

Il server vecchio, ancora efficiente, è stato configurato come unità di REPLICA, questo permette all'Ente di avere una unità di produzione allineata e pronta l'uso in caso di crash del sistema principale garantendo la Continuità Operativa nei servizi essenziali.

2 Network

Pur nella sua semplicità, il sistema di network-LAN è costituito da switch managed che permettono l'implementazione di nuove configurazioni.

Sono stati inseriti nuovi switch nella sala server con due dorsali che collegano il rack del server con il rack del centro stella posto al piano terra.

Tale implementazione rafforza la sicurezza e la gestione del network.

La rete fisica dati è stata realizzata molti anni fa quindi comincia a risentire dell'obsolescenza delle terminazioni e non potendo rifare in toto la cablatura si renderebbe necessario sostituire tutte le terminazioni presenti negli armadi rack con conseguente aggiornamento delle strutture Patch Panel ed i cavi di raccordo Patch Cord.

Inoltre sarebbe opportuno sostituire tutte le strutture patch cord presenti dalle prese a muro ai PC con mappatura e rinumerazione delle stesse con realizzazione dello schema di networking al fine di una individuazione rapida e precisa delle terminazioni LAN.

Sono presenti alcuni switch di teminazione per sdoppiare le prese, queste situazioni vanno eliminate creando le prese necessarie al fine di avere un network omogeneo.

3 SICUREZZA – FIREWALL – WEB FILTERING

E' presente ed in funzione un sistema di Web Filtering e firewall Pf Sense.

4 Backup – Disaster Recover

I processi di backup vengono regolarmente eseguiti, ed abbiamo attivato un sistema di notifiche che ci permette di sorvegliare quotidianamente l'andamento dei backup.

Attualmente i sistemi di Disaster Recovery sono composti da:

a – n. 01 NAS primario presente presso il rack sito nella sala ced,

b – n. 01 NAS secondario sito nel rack presente presso i locali della Protezione Civile.

c – n. 02 HDD esterni, aggiornati con dischi di più ampia capacità, per eseguire copie di backup offline come previsto dalle misure minime AgID

Si consiglia di attivare un sistema di Backup totale presso una struttura certificata Cloud al fine di completare i livelli di sicurezza.

Tutto il sistema di backup viene eseguito con cadenze giornaliere, settimanali e mensili a seconda della programmazione ed ha minimo 30 punti ripristino (la soglia minima prevista è 15 punti).

5 CLIENT

I Client presenti sono mediamente efficienti a livello di prestazioni.

Tutti i client sono con sistema oprativo Windows 10 e sono upgradati con con l'adozione di dischi fissi di tipo SSD e l'espansione della ram ad 8 GB.

Al fine di ottimizzare la rotazione dei client si consiglia di impostare un piano di sostituzione programmata anche relativamente ai monitor per i prossimi anni al fine di mantenere efficiente il parco Client.

6 LICENZE SOFTWARE OFFICE AUTOMATION

Tutte le postazioni sono dotate di nuove licenze Office 2019 originali.

7 Misure Minime

Oltre alle indicazioni sopra descritte da implementare, stiamo procedendo alle attività inerenti il rispetto delle "Misure minime di sicurezza ICT per le pubbliche amministrazioni".

8 MAIL

Si è provveduto alla razionalizzazione delle caselle mail con conseguente passaggio dal sistema POP3 al sistema IMAP e/o WEB MAIL, ciò comporta un vantaggio significativo a livello di interoperabilità, una razionalizzazione delle mail generiche d'ufficio, la possibilità di usufruire delle mail anche al di fuori dell'ufficio e semplifica le attività di backup delle mail.

9 SISTEMA TELEFONICO

Il sistema telefonico dell'Ente è ancora di tipo analogico.

Si consiglia il passaggio alla tecnologia digitale VOIP che renderebbe possibile mettere a disposizione dell'ente un sistema moderno anche in ottica smar-working e razionalizzare al ribasso le spese telefoniche.

10 CONNETTIVITA'

Si è provvedendo a potenziare la connettività presente con l'adozione di 2 linee a fibra FTTCAB fino a 100 che permettono un buon aumento delle prestazioni.

11 SMART WORKING

L'Ente si è dotato di una piattaforma di smart-working che permette agli usufruitori di operare in totale autonomia al di fuori dei canonici luoghi di lavoro usufruendo di tutte le funzionalità presenti in ufficio. Tale sistema presenta buoni canoni di sicurezza ed è indipendente dagli apparati utilizzati da remoto.

Il completamento delle attività per l'adozione del sistema WEB MAIL e l'utilizzo delle funzionalità previste da un nuovo sistema telefonico permetterebbe ai funzionari del Comune di avere tutti gli strumenti necessari al lavoro in qualsiasi luogo si trovino.

12 RETE WIFI INTERNA

Sono stati sostituiti due access point obsoleti con apparati di nuova generazione presenti nell'impianto Wi-Fi interno a copertura parziale del municipio .

Tali apparati sono gestiti con un idoneo sistema di Controller a livello server che permettono la gestione e controllo della rete.

Questo tipo di configurazione prevede quindi una separazione tra la rete degli uffici comunali e la rete Wi-Fi, utilizzata anche con dispositivi non gestiti dal comune e prevede un sistema di autenticazione controllata degli utenti.

Tale configurazione permette di gestire più SSID e di creare una rete „guest" quindi separata e isolata rispetto alla rete del Comune e con un sistema di autenticazione tracciabile e gestibile.

13 Adempimenti Piano Triennale AgID 2020-2022 inerenti la materia della Cyber Security.

Nello specifico il piano prevede alcune fondamentali scadenze:

[1] Entro dicembre 2021: le PA valutano l'utilizzo del tool di Cyber Risk Assessment per l'analisi del rischio e la redazione del Piano dei trattamenti

[2] Entro marzo 2022: le PA definiscono, sulla base di quanto proposto dal RTD, all'interno dei piani di formazione del personale, interventi sulle tematiche di Cyber Security Awareness

[3] Entro giugno 2022: le PA si adeguano alle Misure Minime di Sicurezza ICT per le pubbliche amministrazioni aggiornate

Tali adempimenti, in capo al Responsabile per la Transizione Digitale, oltre ad essere un obbligo che può essere adempiuto formalmente con una serie di attività, sono indubbiamente un opportunità per una seria ed approfondita valutazione del reale stato della sicurezza dei propri

sistemi, elemento essenziale per Enti che basano i propri asset informativi quasi completamente su sistemi informatizzati.

Si consiglia di integrare le attività previste con più approfondite analisi effettuate con strumenti automatizzati e con l'impiego di specialisti altamente qualificati, secondo i criteri e le specifiche di una corretta applicazione dei principi di Cyber-security che impone una costante applicazione di attività e verifica, secondo il principio del ciclo PDCA (Plan Do Check Act), che di fatto non avrà mai termine nel tempo.

Per tale motivo si consiglia, ovvero la pianificazione e ripetizione nel tempo di tutte le attività necessarie per il mantenimento di uno stato eccellente della sicurezza.

Le attività potrebbero essere effettuate in:

1 *Esecuzione dei test di Security*

1.1 *Esecuzione di test di vulnerability assessment interni*

Esecuzione di test interni alla rete LAN dell'Ente, finalizzati ad individuare le vulnerabilità di: PC, apparati di rete, server, host. con l'utilizzo di tool di analisi specifici che saranno gestiti da apposita appliance o VM installata all'interno.

1.2 *Esecuzione di test di vulnerability assessment da esterno*

Esecuzione di test dall'esterno sugli indirizzi IP pubblici con servizi esposti

1.3 *Esecuzione di penetration test*

Esecuzione di penetration test dall'esterno per la valutazione dello stato di protezione della rete

1.4 Applicazione del tool di Cyber Risk Assessment AgID

2 *Predisposizione del piano di formazione del personale*

2.1 Adozione di un completo piano di e-learning tramite piattaforma dedicata per la formazione a tutti i livelli. Test on-line di verifica di avvenuta comprensione